

National Cyber Alert System

[Archive](#)

Cyber Security Bulletin SB09-348

Vulnerability Summary for the Week of December 7, 2009

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
activewebswares -- active_bids	Multiple SQL injection vulnerabilities in ActiveWebSoftwares Active Bids allow remote attackers to execute arbitrary SQL commands via (1) the catid parameter in the PATH_INFO to the default URI or (2) the catid parameter to default.asp. NOTE: this might overlap CVE-2009-0429.3. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-12-08	7.5	CVE-2009-4229 XF BID
adobe -- adobe_air adobe -- flash_player	Heap-based buffer overflow in Adobe Flash Player before 10.0.42.34 and Adobe AIR before 1.5.3 allows remote attackers to execute arbitrary code via crafted dimensions of JPEG data in an SWF file.	2009-12-10	9.3	CVE-2009-3794 CERT
adobe -- adobe_air	Adobe Flash Player before 10.0.42.34 and Adobe AIR before 1.5.3 might allow attackers to	2009-12-	0.0	CVE-2009-0766

adobe -- flash_player	execute arbitrary code via unspecified vectors, related to a "data injection vulnerability."	10	9.3	3/90 CERT
adobe -- adobe_air adobe -- flash_player	Adobe Flash Player 10.x before 10.0.42.34 and Adobe AIR before 1.5.3 might allow attackers to execute arbitrary code via unspecified vectors that trigger memory corruption.	2009-12-10	9.3	CVE-2009-3797 CERT
adobe -- adobe_air adobe -- flash_player	Adobe Flash Player before 10.0.42.34 and Adobe AIR before 1.5.3 might allow attackers to execute arbitrary code via unspecified vectors that trigger memory corruption.	2009-12-10	9.3	CVE-2009-3798 CERT
adobe -- adobe_air adobe -- flash_player	Integer overflow in the Verifier::parseExceptionHandlers function in Adobe Flash Player before 10.0.42.34 and Adobe AIR before 1.5.3 allows remote attackers to execute arbitrary code via an SWF file with a large exception_count value that triggers memory corruption, related to "generation of ActionScript exception handlers."	2009-12-10	9.3	CVE-2009-3799 CERT
adobe -- adobe_air adobe -- flash_player	Multiple unspecified vulnerabilities in Adobe Flash Player before 10.0.42.34 and Adobe AIR before 1.5.3 allow attackers to cause a denial of service (application crash) or possibly execute arbitrary code via unknown vectors.	2009-12-10	9.3	CVE-2009-3800 CERT
adobe -- adobe_air adobe -- flash_player	Unspecified vulnerability in the Flash Player ActiveX control in Adobe Flash Player before 10.0.42.34 and Adobe AIR before 1.5.3 on Windows allows remote attackers to obtain the names of local files via unknown vectors. NOTE: this vulnerability exists because of an incomplete fix for CVE-2008-4820.	2009-12-10	7.1	CVE-2009-3951 CERT
apple -- mac_os_x apple -- mac_os_x_server	Java for Mac OS X 10.5 before Update 6 and 10.6 before Update 1 accepts expired certificates for applets, which makes it easier for remote attackers to execute arbitrary code via an applet.	2009-12-08	7.5	CVE-2009-2843 BID CONFIRM CONFIRM APPLE APPLE
basic-cms -- sweetrice	Directory traversal vulnerability in as/lib/plugins.php in SweetRice 0.5.3 and earlier allows remote attackers to include and execute arbitrary local files via .. (dot dot) in the plugin parameter.	2009-12-08	7.5	CVE-2009-4231 MISC

ca -- etrust_pestpatrole_ppctl.dll_activex	Stack-based buffer overflow in the PestPatrol ActiveX control (ppctl.dll) 5.6.7.9 in CA eTrust PestPatrol allows remote attackers to execute arbitrary code via a long argument to the Initialize method.	2009-12-08	9.3	CVE-2009-4225 XF BID MISC MISC
corel -- paint_shop_pro	Stack-based buffer overflow in Jasc Paint Shop Pro 8.10 (aka Corel Paint Shop Pro) allows user-assisted remote attackers to execute arbitrary code via a crafted PNG file. NOTE: this might be the same issue as CVE-2007-2366.	2009-12-09	9.3	CVE-2009-4251 XF VUPEN BID MISC SECUNIA OSVDB MISC
denton_woods -- devil	Stack-based buffer overflow in the GetUID function in src-IL/src/il_dicom.c in DevIL 1.7.8 allows remote attackers to cause a denial of service (application crash) or execute arbitrary code via a crafted DICOM file.	2009-12-08	9.3	CVE-2009-3994 CONFIRM
findmysoft -- alefmentor	Multiple SQL injection vulnerabilities in course.php in AlefMentor 2.0 and 2.2 allow remote attackers to execute arbitrary SQL commands via the (1) cont_id and (2) courc_id parameters in a pregled action. NOTE: some of these details are obtained from third party information.	2009-12-09	7.5	CVE-2009-4256 XF MISC SECUNIA
frank_yaul -- corehttp	Off-by-one error in src/http.c in CoreHTTP 0.5.3.1 and earlier allows remote attackers to cause a denial of service or possibly execute arbitrary code via an HTTP request with a long first line that triggers a buffer overflow. NOTE: this vulnerability reportedly exists because of an incorrect fix for CVE-2007-4060.	2009-12-08	7.5	CVE-2009-3586 MISC
gianni_tommasi -- kr-php_web_content_server	PHP remote file inclusion vulnerability in adm/krgourl.php in KR-Web 1.1b2 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the DOCUMENT_ROOT parameter.	2009-12-07	7.5	CVE-2009-4223 XF MISC
haihaisoft -- haihaisoft_universal_player	Stack-based buffer overflow in the MYACTIVE.MyActiveXCtrl.1 ActiveX control in MyActiveX.ocx 1.4.8.0 in Haihaisoft Universal Player allows remote attackers to execute arbitrary code via a long	2009-12-07	9.3	CVE-2009-4219 MISC SECUNIA

	URL property value. NOTE: some of these details are obtained from third party information.			SECUNIA
harold_bakker -- hb-ns	Harold Bakker's Newscript HB-NS 1.3 allows remote attackers to obtain access to the admin control panel via a direct request to admin.php.	2009-12-10	7.5	CVE-2009-4262 XF MISC
hp -- openview_data_protector_application_recovery_manager	Unspecified vulnerability in HP OpenView Data Protector Application Recovery Manager 5.0 and 6.0 allows remote attackers to cause a denial of service via unknown vectors.	2009-12-08	7.8	CVE-2009-3844 BID HP HP
hp -- openview_network_node_manager	The port-3443 HTTP server in HP OpenView Network Node Manager (OV NNM) 7.01, 7.51, and 7.53 allows remote attackers to execute arbitrary commands via shell metacharacters in the hostname parameter to unspecified Perl scripts.	2009-12-10	10.0	CVE-2009-3845 HP HP
hp -- openview_network_node_manager	Multiple heap-based buffer overflows in ovlogin.exe in HP OpenView Network Node Manager (OV NNM) 7.01, 7.51, and 7.53 allow remote attackers to execute arbitrary code via a long (1) userid or (2) passwd parameter.	2009-12-10	10.0	CVE-2009-3846 HP HP
hp -- openview_network_node_manager	Unspecified vulnerability in HP OpenView Network Node Manager (OV NNM) 7.01, 7.51, and 7.53 allows remote attackers to execute arbitrary code via unknown vectors.	2009-12-10	10.0	CVE-2009-3847 HP HP
hp -- openview_network_node_manager	Stack-based buffer overflow in nnmRptConfig.exe in HP OpenView Network Node Manager (OV NNM) 7.01, 7.51, and 7.53 allows remote attackers to execute arbitrary code via a long Template parameter, related to the vsprintf function.	2009-12-10	10.0	CVE-2009-3848 HP HP
hp -- openview_network_node_manager	Multiple stack-based buffer overflows in HP OpenView Network Node Manager (OV NNM) 7.01, 7.51, and 7.53 allow remote attackers to execute arbitrary code via (1) a long Template parameter to nnmRptConfig.exe, related to the streat function; or (2) a long Oid parameter to snmp.exe.	2009-12-10	10.0	CVE-2009-3849 HP HP
	Multiple heap-based buffer overflows in ovsessionmgr.exe in			CVE-2009-3850

hp -- openview_network_node_manager	HP OpenView Network Node Manager (OV NNM) 7.01, 7.51, and 7.53 allow remote attackers to execute arbitrary code via a long (1) userid or (2) passwd parameter to ovlogin.exe.	2009-12-10	10.0	CVE-2009-4176 BID HP HP
hp -- openview_network_node_manager	Buffer overflow in webappmon.exe in HP OpenView Network Node Manager (OV NNM) 7.01, 7.51, and 7.53 allows remote attackers to execute arbitrary code via a long HTTP Host header.	2009-12-10	10.0	CVE-2009-4177 HP HP
hp -- openview_network_node_manager	Heap-based buffer overflow in OvWebHelp.exe in HP OpenView Network Node Manager (OV NNM) 7.01, 7.51, and 7.53 allows remote attackers to execute arbitrary code via a long Topic parameter.	2009-12-10	10.0	CVE-2009-4178 BID BUGTRAQ HP HP MISC
hp -- openview_network_node_manager	Stack-based buffer overflow in ovalarm.exe in HP OpenView Network Node Manager (OV NNM) 7.01, 7.51, and 7.53 allows remote attackers to execute arbitrary code via a long HTTP Accept-Language header in an OVABverbose action.	2009-12-10	10.0	CVE-2009-4179 BID HP HP
hp -- openview_network_node_manager	Stack-based buffer overflow in snmpviewer.exe in HP OpenView Network Node Manager (OV NNM) 7.01, 7.51, and 7.53 allows remote attackers to execute arbitrary code via a long HTTP Host header.	2009-12-10	10.0	CVE-2009-4180 BID
hp -- openview_network_node_manager	Stack-based buffer overflow in ovwebsnmpsrv.exe in HP OpenView Network Node Manager (OV NNM) 7.01, 7.51, and 7.53 allows remote attackers to execute arbitrary code via vectors involving the sel and arg parameters to jovgraph.exe.	2009-12-10	10.0	CVE-2009-4181 BID HP HP
hp -- openview_network_node_manager	Stack-based buffer overflow in HP OpenView Network Node Manager (OV NNM) 7.01, 7.51, and 7.53 allows remote attackers to execute arbitrary code via a crafted HTTP request.	2009-12-10	10.0	CVE-2009-0898 HP HP
ibm -- infosphere_information_server	Multiple buffer overflows in unspecified setuid executables in the DataStage subsystem in IBM InfoSphere Information Server 8.1 before FP1 have unknown impact and attack vectors.	2009-12-09	10.0	CVE-2009-4240 XF VUPEN BID OSVDB CONFIRM SECUNIA

ijj -- seil/b1 ijj -- seil/x1 ijj -- seil/x2	Buffer overflow in the URL filtering function in Internet Initiative Japan SEIL/X1, SEIL/X2, and SEIL/B1 firmware 2.40 through 2.51 allows remote attackers to execute arbitrary code via unspecified vectors.	2009-12-10	9.3	CVE-2009-4292 XF VUPEN CONFIRM SECUNIA OSVDB JVNDB JVN
ijj -- seil/b1 ijj -- seil/x1 ijj -- seil/x2	Internet Initiative Japan SEIL/X1, SEIL/X2, and SEIL/B1 firmware 2.30 through 2.51, when NAT is enabled, allows remote attackers to cause a denial of service (system restart) via crafted GRE packets.	2009-12-10	7.1	CVE-2009-4293 XF VUPEN CONFIRM SECUNIA OSVDB JVNDB JVN
itamar_elharar -- com_musicgallery	SQL injection vulnerability in the Itamar Elharar MusicGallery (com_musicgallery) component for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter in an itempage action to index.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-12-07	7.5	CVE-2009-4217 BID
jiros -- jbsx	Multiple SQL injection vulnerabilities in files/login.asp in JiRo's Banner System eXperience (JBSX) allow remote attackers to execute arbitrary SQL commands via the (1) admin or (2) password field, a related issue to CVE-2007-6091. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-12-07	7.5	CVE-2009-4218 XF BID
klinza -- klinza_professional_cms	Directory traversal vulnerability in funzioni/lib/menulast.php in klinza professional cms 5.0.1 and earlier allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the LANG parameter.	2009-12-07	9.3	CVE-2009-4216 XF BID MISC
linux -- kernel	The ip_frag_reasm function in ipv4/ip_fragment.c in Linux kernel 2.6.32-rc8, and possibly earlier versions, calls IP_INC_STATS_BH with an incorrect argument, which allows remote attackers to cause a denial of service (NULL pointer dereference and hang) via long IP packets, possibly related to	2009-12-08	7.8	CVE-2009-1298 FEDORA FEDORA CONFIRM OSVDB SECUNIA CONFIRM

	the ip_defrag function.			
microsoft -- office_project microsoft -- project_portfolio_server microsoft -- project_server	Microsoft Project 2000 SR1 and 2002 SP1, and Office Project 2003 SP3, does not properly handle memory allocation for Project files, which allows remote attackers to execute arbitrary code via a malformed file, aka "Project Memory Validation Vulnerability."	2009-12-09	9.3	CVE-2009-0102 MS
microsoft -- windows_server_2008 microsoft -- windows_vista	The Internet Authentication Service (IAS) in Microsoft Windows Vista SP2 and Server 2008 SP2 does not properly validate MS-CHAP v2 Protected Extensible Authentication Protocol (PEAP) authentication requests, which allows remote attackers to execute arbitrary code via crafted structures in a malformed request, aka "Internet Authentication Service Memory Corruption Vulnerability."	2009-12-09	10.0	CVE-2009-2505 MS
microsoft -- office_converter_pack microsoft -- office_word microsoft -- works microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_xp	The text converters in Microsoft Office Word 2002 SP3 and 2003 SP3; Works 8.5; Office Converter Pack; and WordPad in Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 do not properly parse Word 97 documents, which allows remote attackers to execute arbitrary code via a crafted document, aka "WordPad and Office Text converter Memory Corruption Vulnerability."	2009-12-09	9.3	CVE-2009-2506 MS
microsoft -- windows_server_2003 microsoft -- windows_server_2008	Active Directory Federation Services (ADFS) in Microsoft Windows Server 2003 SP2 and Server 2008 Gold and SP2 does not properly validate headers in HTTP requests, which allows remote authenticated users to execute arbitrary code via a crafted request to an IIS web server, aka "Remote Code Execution in ADFS Vulnerability."	2009-12-09	9.0	CVE-2009-2509 MS
microsoft -- ie microsoft -- windows_2000 microsoft -- windows_7 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Microsoft Internet Explorer 8 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing an object that (1) was not properly initialized or (2) is deleted, leading to memory corruption, aka "Uninitialized Memory Corruption Vulnerability," a different vulnerability than CVE-2009-	2009-12-09	9.3	CVE-2009-3671 MS

	3674.			
microsoft -- ie microsoft -- windows_2000 microsoft -- windows_7 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Microsoft Internet Explorer 7 and 8 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing an object that (1) was not properly initialized or (2) is deleted, leading to memory corruption, aka "Uninitialized Memory Corruption Vulnerability."	2009-12-09	9.3	CVE-2009-3673 MS
microsoft -- ie microsoft -- windows_2000 microsoft -- windows_7 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Microsoft Internet Explorer 8 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing an object that (1) was not properly initialized or (2) is deleted, leading to memory corruption, aka "Uninitialized Memory Corruption Vulnerability," a different vulnerability than CVE-2009-3671.	2009-12-09	9.3	CVE-2009-3674 MS
microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	The Internet Authentication Service (IAS) in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold and SP1, and Server 2008 Gold does not properly verify the credentials in an MS-CHAP v2 Protected Extensible Authentication Protocol (PEAP) authentication request, which allows remote attackers to access network resources via a malformed request, aka "MS-CHAP Authentication Bypass Vulnerability."	2009-12-09	10.0	CVE-2009-3677 MS
novell -- iprint_client	Stack-based buffer overflow in ienipp.ocx in Novell iPrint Client 5.30, and possibly other versions before 5.32, allows remote attackers to execute arbitrary code via a long target-frame parameter.	2009-12-08	9.3	CVE-2009-1568 VUPEN BID CONFIRM
novell -- iprint	Multiple stack-based buffer overflows in Novell iPrint Client 4.38, 5.30, and possibly other versions before 5.32 allow remote attackers to execute arbitrary code via vectors related to (1) Date and (2) Time.	2009-12-08	9.3	CVE-2009-1569 VUPEN BID CONFIRM
pandasecurity -- panda_antivirus pandasecurity -- panda_global_protection pandasecurity -- panda_internet_security	Panda Global Protection 2010, Internet Security 2010, and Antivirus Pro 2010 use weak permissions (Everyone: Full Control) for the product files, which allows local users to gain	2009-12-07	7.2	CVE-2009-4215 VUPEN GATEWAY

	privileges by replacing executables with Trojan horse programs.			CONFIRM
pointdev -- ideal_administration_2009	Stack-based buffer overflow in Ideal Administration 2009 9.7.1, and possibly other versions, allows remote attackers to execute arbitrary code via a long Computer value in an .ipj project file.	2009-12-10	9.3	CVE-2009-4265 SECUNIA MISC MISC
ptcpay -- gen3_forum_1.3	SQL injection vulnerability in main_forum.php in PTCPay GeN3 forum 1.3 allows remote attackers to execute arbitrary SQL commands via the cat parameter.	2009-12-10	7.5	CVE-2009-4263 XF MISC
raphael_mazoyer -- pointcomma	PHP remote file inclusion vulnerability in includes/classes/pctemplate.php in PointComma 3.8b2 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the pcConfig[smartyPath] parameter.	2009-12-07	7.5	CVE-2009-4220 XF MISC MISC
ruven_pillay -- iipimage_server	Multiple stack-based buffer overflows in src/Task.cc in the FastCGI program in IIPImage Server before 0.9.8 might allow remote attackers to execute arbitrary code via vectors associated with crafted arguments to the (1) RGN::run, (2) JTLS::run, or (3) SHD::run function. NOTE: some of these details are obtained from third party information.	2009-12-08	10.0	CVE-2009-4230 SECUNIA CONFIRM CONFIRM
smartisoft -- phpbazar	SQL injection vulnerability in classified.php in phpBazar 2.1.1fix and earlier allows remote attackers to execute arbitrary SQL commands via the catid parameter, a different vector than CVE-2008-3767.	2009-12-07	7.5	CVE-2009-4221 XF BID MISC MISC
smartisoft -- phpbazar	phpBazar 2.1.1fix and earlier does not require administrative authentication for admin/admin.php, which allows remote attackers to obtain access to the admin control panel via a direct request.	2009-12-07	7.5	CVE-2009-4222 BID MISC
sun -- opensolaris	Race condition in the IP module in the kernel in Sun OpenSolaris snv_106 through snv_124 allows remote attackers to cause a denial of service (NULL pointer dereference and panic) via unspecified vectors related to the (1) tcp_do_getsockname or (2)	2009-12-08	7.1	CVE-2009-4226 SUNALERT

tcp_do_getpeername function.

[Back to top](#)**Medium Vulnerabilities**

Primary Vendor -- Product	Description
aroundme -- aroundme barnraiser -- aroundme	PHP remote file inclusion vulnerability in components/core/connect.php in AROUNDMe 1.1 and earlier, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the language_path parameter.
basic-cms -- sweetrice	Multiple PHP remote file inclusion vulnerabilities in SweetRice 0.5.4, 0.5.3, and earlier allow remote attackers to execute arbitrary PHP code via a URL in the root_dir parameter to (1) _plugin/subscriber/inc/post.php and (2) as/lib/news_modify.php.
ca -- service_desk	Cross-site scripting (XSS) vulnerability in the web interface in CA Service Desk 12.1 allows remote attackers to inject arbitrary web script or HTML via an unspecified parameter.
cutephp -- cutenews korn19 -- utf-8_cutenews	Multiple cross-site scripting (XSS) vulnerabilities in CutePHP CuteNews 1.4.6 and UTF-8 CuteNews before 8b allow remote attackers to inject arbitrary web script or HTML via (1) the result parameter to register.php; (2) the user parameter to search.php; the (3) cat_msg, (4) source_msg, (5) postponed_selected, (6) unapproved_selected, and (7) news_per_page parameters in a list action to the editnews module of index.php; and (8) the link tag in news comments. NOTE: some of the vulnerabilities require register_globals to be enabled and/or magic_quotes_gpc to be disabled.
ec-cube -- ec-cube_ver2	The process function in data/class/pages/admin/customer/LC_Page_Admin_Customer_SearchCustomer.php in EC-CUBE Ver2 2.4.0 RC1 through 2.4.1, and Community Edition r18068 through r18428, allows remote attackers to obtain sensitive information (customer data) via unknown vectors related to sessions.
ibm -- communications_enabled_applications ibm -- websphere_application_server	Feature Pack for Communications Enabled Applications (CEA) before 1.0.0.1 for IBM WebSphere Application Server 7.0.0.7 uses predictable session values, which allows man-in-the-middle attackers to spoof a collaboration session by guessing the value.
ibm -- infosphere_information_server	Cross-site scripting (XSS) vulnerability in the Web console in IBM InfoSphere Information Server 8.1 before FP1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
image-host-script -- image_hosting_script	Cross-site scripting (XSS) vulnerability in images.php in Image Hosting Script DPI 1.1 Final (1.1F) allows remote attackers to inject arbitrary web script or HTML via the date parameter. NOTE: some of these details are obtained from third party information.
jonijnm -- com_kide	The Kide Shoutbox (com_kide) component 0.4.6 for Joomla! does not properly perform authentication, which allows remote attackers to post messages with an arbitrary account name via an insertar action to index.php. NOTE: the provenance of

	this information is unknown; the details are obtained solely from third party information.
micronet -- network_access_controller_sp1910	Cross-site scripting (XSS) vulnerability in loginpages/error_user.shtml on the Micronet Network Access Controller SP1910 allows remote attackers to inject arbitrary web script or HTML via the msg parameter.
microsoft -- windows_server_2003 microsoft -- windows_server_2008	The single sign-on implementation in Active Directory Federation Services (ADFS) in Microsoft Windows Server 2003 SP2 and Server 2008 Gold and SP2 does not properly remove credentials at the end of a network session, which allows physically proximate attackers to obtain the credentials of a previous user of the same web browser by using data from the browser's cache, aka "Single Sign On Spoofing in ADFS Vulnerability."
microsoft -- windows_2000 microsoft -- windows_2003_server microsoft -- windows_xp	LSASS.exe in the Local Security Authority Subsystem Service (LSASS) in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 allows remote authenticated users to cause a denial of service (CPU consumption) via a malformed ISAKMP request over IPsec, aka "Local Security Authority Subsystem Service Resource Exhaustion Vulnerability."
nathan_haug -- webform	Cross-site scripting (XSS) vulnerability in the Webform module 5.x before 5.x-2.7 and 6.x before 6.x-2.7, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via a submission.
ntp -- ntp	ntp_request.c in ntpd in NTP before 4.2.4p8, and 4.2.5, allows remote attackers to cause a denial of service (CPU and bandwidth consumption) by using MODE_PRIVATE to send a spoofed (1) request or (2) response packet that triggers a continuous exchange of MODE_PRIVATE error responses between two NTP daemons.
phpee -- power_phlogger	Cross-site scripting (XSS) vulnerability in dspStats.php in PowerPhlogger 2.2.5 allows remote attackers to inject arbitrary web script or HTML via the edit parameter.
phpee -- power_phlogger	PowerPhlogger 2.2.5 allows remote attackers to obtain sensitive information via a direct request to (1) edCss.inc.php, (2) foot.inc.php, (3) get_esscolors.inc.php, (4) head.inc.php, (5) head_stuff.inc.php, (6) loglist.inc.php, and (7) phlogger_send.inc.php in include/, which reveals the installation path in an error message.
ruby_on_rails -- ruby_on_rails	Cross-site scripting (XSS) vulnerability in the strip_tags function in Ruby on Rails before 2.2.s, and 2.3.x before 2.3.5, allows remote attackers to inject arbitrary web script or HTML via vectors involving non-printing ASCII characters, related to HTML::Tokenizer and actionpack/lib/action_controller/vendor/html-scanner/html/node.rb.
teamst -- testlink	Multiple SQL injection vulnerabilities in TestLink before 1.8.5 allow remote authenticated users to execute arbitrary SQL commands via (1) the Test Case ID field to lib/general/navBar.php or (2) the logLevel parameter to lib/events/eventviewer.php.
tim_hockin -- acpid	A certain Red Hat patch for acpid 1.0.4 effectively triggers a call to the open function with insufficient arguments, which might allow local users to leverage weak permissions on /var/log/acpid, and obtain sensitive information by reading this file, cause a denial of service by overwriting this file, or gain privileges by executing this file.
	acpid 1.0.4 sets an unrestrictive umask, which might allow local users to leverage

tim_hockin -- acpid	weak permissions on /var/log/acpid, and obtain sensitive information by reading this file or cause a denial of service by overwriting this file, a different vulnerability than CVE-2009-4033.
xfig -- xfig	Stack-based buffer overflow in the read_1_3_textobject function in f_readold.c in Xfig 3.2.5b and earlier, and in the read_textobject function in read1_3.c in fig2dev in Transfig 3.2.5a and earlier, allows remote attackers to execute arbitrary code via a long string in a malformed .fig file that uses the 1.3 file format. NOTE: some of these details are obtained from third party information.
xfig -- xfig	Stack consumption vulnerability in u_bound.c in Xfig 3.2.5b and earlier allows remote attackers to cause a denial of service (application crash) via a long string in a malformed .fig file that uses the 1.3 file format, possibly related to the readfp_fig function in f_read.c.
yabsoft -- advanced_image_hosting_script	Cross-site scripting (XSS) vulnerability in search.php in YABSoft Advanced Image Hosting (AIH) Script 2.2, and possibly 2.3, allows remote attackers to inject arbitrary web script or HTML via the text parameter.
youjoomla -- yj_whois	Cross-site scripting (XSS) vulnerability in modules/mod_yj_whois.php in the YJ Whois component 1.0x and 1.5.x for Joomla! allows remote attackers to inject arbitrary web script or HTML via the domain parameter to index.php. NOTE: some of these details are obtained from third party information.
youjoomla -- you!hostit!	Cross-site scripting (XSS) vulnerability in the You!Hostit! template 1.0.1 for Joomla! allows remote attackers to inject arbitrary web script or HTML via the created_by_alias parameter in index.php.

[Back to top](#)

Low Vulnerabilities					
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info	
cutephp -- cutenews	Multiple cross-site scripting (XSS) vulnerabilities in CutePHP CuteNews 1.4.6, when register_globals is enabled and magic_quotes_gpc is disabled, allow remote attackers to inject arbitrary web script or HTML via the (1) lastusername and (2) mod parameters to index.php; and (3) the title parameter to search.php.	2009-12-09	2.6	CVE-2009-4249 XF XF XF BID BUGTRAQ MISC	
teamst -- testlink	Multiple cross-site scripting (XSS) vulnerabilities in TestLink before 1.8.5 allow remote attackers to inject arbitrary web script or HTML via (1) the req parameter to login.php, and allow remote authenticated users to inject arbitrary web script or HTML via (2) the key parameter to lib/general/staticPage.php, (3) the tableName parameter to lib/attachments/attachmentupload.php, or the (4) startDate, (5) endDate, or (6) logLevel parameter to lib/events/eventviewer.php; (7) the search_notes_string parameter to lib/results/resultsMoreBuilds_buildReport.php; or the (8) expected_results, (9) name, (10) steps, or (11) summary parameter in a find action to lib/testcases/searchData.php,	2009-12-10	3.5	CVE-2009-4237 CONFIRM BID	

related to lib/functions/database.class.php.

[Back to top](#)

Last updated December 14, 2009

 Print This Document